An Exploration of the Physics of Entangled Photon States, and their Utility in Key Distribution Protocols

Noah Kriss, Liam Gallagher, Jacob Faller, Jason Zhao, John Macaulay

[1] Department of Physics, Engineering Physics & Astronomy, Queen's University, Kingston, ON, Canada

Submitted December 6th, 2022

Abstract

In this experiment, a partial implementation of the BB84 protocol (Charles Bennett and Gilles Brassard, 1984) is conducted to study the nature of entangled photons. A 405 nm, 50 mW laser was used to shoot a beam of photons into a Barium Borate crystal This created two beams of IR, polarization entangled photons, which were detected using two single photon detectors and an Altera FPGA for coincidence counts. By changing the orientation of two half-wave plates, one at each detector, one can simulate the transfer of bits between two parties, Alice, and Bob. By introducing an eavesdropper in the form of a quartz plate on a rotating mount, we were able to show that the eavesdropper alters the state of the photons such that there is a roughly 50% reduction in coincidence counts, agreeing with our predictions.

---

1. Introduction

Cryptography is the study of transmitting information across public channels, such that the chances of eavesdroppers obtaining the information is minimal. This means that if someone was able to intercept the exchange, there should be no way of reading the data.

A crucial stage of ensuring the secure transfer of information is private key exchange. The main methods currently used to do this are the Diffie-Hellman Algorithm, Elliptic Curve Algorithm, and RSA encryption. All three of these methods are secure due to the lack of an efficient solution to the Discrete Logarithm Problem with classical computers [1]. Currently these methods of encryption are secure, however with the rapid advancement of quantum computers, this will not always be the case. Once quantum computers reach approximately 3000 qubits, they will theoretically be able to implement Shor's algorithm to factor prime numbers [2]. Assuming no major barriers or setbacks in the development of qubits, it seems inevitable that most current methods of private key transfer protocols will become useless. Luckily, this problem can be solved with Quantum Cryptography.

Quantum Key Distribution (QKD) is built on an extremely fundamental concept in quantum mechanics, decoherence [3]. This describes the effects of quantum particles interactions with their environment, and specifically detectors. When measurements are made on particles, their state irreversibly changes. By using the states of quantum particles to carry information from the sender to the receiver, if any of the states are measured enroute to the intended receiver, then the two users communicating will be able to

identify that eavesdropping took place. A comprehensive protocol for the transfer of private keys using quantum states was developed in 1984 and is referred to as the BB84 protocol. This protocol involves encoding the secret key into binary and then encoding each bit into the polarization of a photon [4]. If a secret key can successfully be transferred between two parties, which we will refer to as Alice and Bob, then they can communicate with no risk of an eavesdropper, Eve, gaining access to the data being transferred.

The goal of this experiment is to create the quantum states necessary for the BB84 protocol, and to show that an eavesdropper can be detected through analysis of coincidence counts. These ''Qubit" states are created by passing a beam of UV photons with a wavelength of 405 nm through a double Barium Borate (BBO) crystal resulting in spontaneous parametric down conversion. Spontaneous Parametric Down Conversion (SPDC) is a process in which a single photon can be split into a pair of photons each with half the wavelength of the incident photon. In this experiment, a double type-I BBO crystal was used as an efficient source of SPDC. This is two BBO crystals at 90 degrees to each other,

The two photons which leave the BBO crystal are referred to as the signal (s) and idler (i) photons and go through the following state change when SPDC occurs:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|V\rangle + |H\rangle) \rightarrow \frac{1}{\sqrt{2}}(|V\rangle_s|V\rangle_i + |H\rangle_s|H\rangle_i) \quad (1)$$

On the left side of the equation, we have a photon in superposition of the Vertical and Horizontal Polarization states which was created by using a half wave plate set at 22.5 degrees. This rotates the initially vertically polarized pump beam from the laser to be at 45 degrees relative to the BBO crystal axis. One in every approximately 10^6 photons are then transformed into an entangled state as shown on the right side. We will refer to this state, $|\psi\rangle$, as being in the horizontal-vertical basis, H-V.

The photons form the following cone as they are emitted from the BBO looking into the path of the laser. Each of these two IR photon beams will travel to either Alice or Bob, where their polarizations are measured with a Thompson Prism.

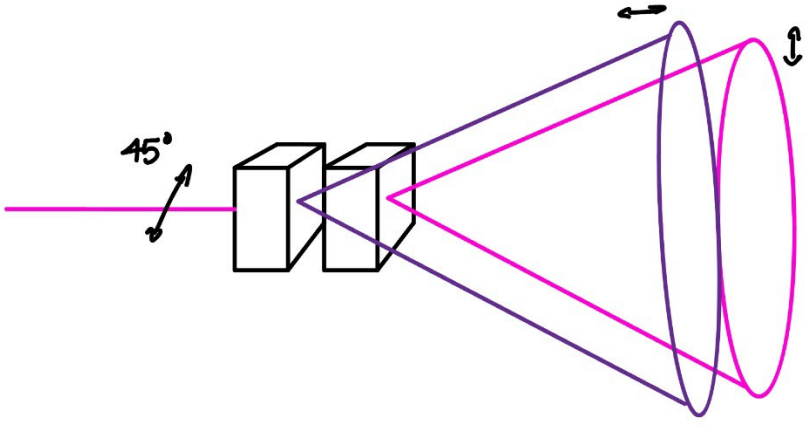

Figure 1 - Cones of Polarized Light emitted by the BBO Crystals

The red dots indicate the locations of the entangled photon beams, and the violet circle is the unaffected UV photons. By placing single photon detectors at the points shown in red, we can detect the entangled photons as given by equation 1.

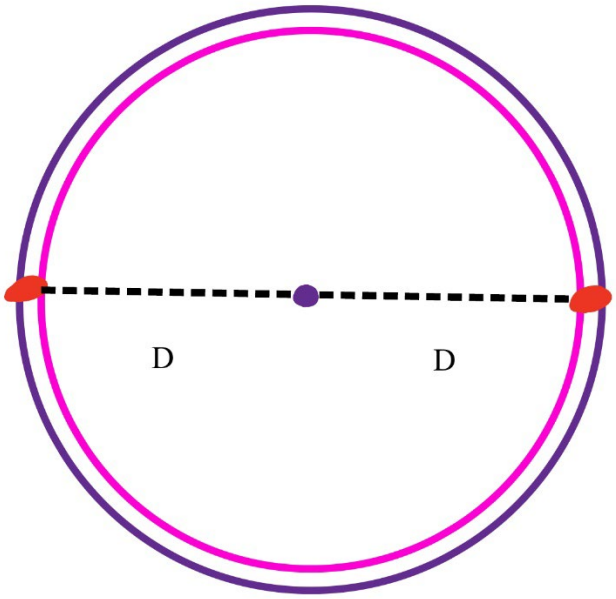

Figure 2 - Measurement locations

D is given by the following equation: $D = Rsin(\theta)$.

To ensure that the detected photons are in fact the entangled photons from the BBO, a coincidence program was used with $\Delta t = 40\ ns$. If two photons were received within a 40 ns period, they are assumed to be entangled photons. To account for errors, the number of photons being detected at each individual detector is used in an accidentals counter and subtracted from the total counts. Further information on the accidental counter can be found below in the data subsection.

By introducing an eavesdropper in the form of a quartz crystal, the entangled photons decohere and become two independent states. The purpose of our experiment is twofold; firstly, we show the entanglement of the photon pairs by changing the measurement basis of Alice and Bob's detectors. Secondly, we show that the interaction of eavesdropping results in a change of the polarization states, therefore reducing the number of coincidence counts, allowing for the detection of Eve.

2. Model and Predictions

Investigating the effect of measurement and differing measurement basis on entangled photon pairs requires us to define the polarization states we are using. The light will be in either the $|V\rangle, |H\rangle, |D\rangle$ or $|A\rangle$ state which, for our purposes, correspond to bits 0 and 1 as $|V\rangle, |D\rangle$ = "1"and $|H\rangle, |A\rangle$ = "0". The states are graphically represented as shown in Figure 3.

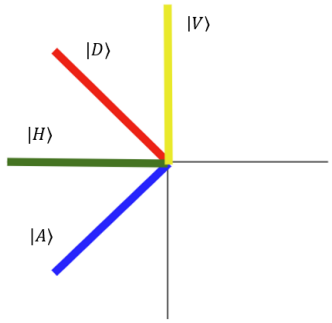

Figure 3: The $|V\rangle, |H\rangle, |D\rangle, |A\rangle$ basis.

We can then define each state as a composite of two orthogonal states which are 45° away.

$$|V\rangle = \frac{1}{\sqrt{2}}(|D\rangle - |A\rangle) \tag{2}$$

$$|H\rangle = \frac{1}{\sqrt{2}}(|D\rangle + |A\rangle) \tag{3}$$

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \tag{4}$$

$$|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \tag{5}$$

The dot products we will be using can be defined as

$$\langle V|V\rangle = \langle H|H\rangle = \langle D|D\rangle = 1 \tag{6}$$

$$\langle V|H\rangle = \langle H|V\rangle = \langle D|A\rangle = 0 \tag{7}$$

$$\langle V|D\rangle = \langle V|A\rangle = \langle D|V\rangle = \langle D|H\rangle = \frac{1}{\sqrt{2}} \tag{8}$$

We must also define measurement operators to operate on our state $|\psi\rangle$, defined in equation 1, which will describe the effect of measuring the polarization of one of our entangled photons. Adapting from reference [5] measuring the photon in the HV and DA basis can be described as

$$\widehat{M}_{HV} = |H\rangle\langle H| - |V\rangle\langle V| \tag{9}$$

$$\widehat{M}_{DA} = |D\rangle\langle D| - |A\rangle\langle A| \tag{10}$$

However, due to having access to only two single photon detectors we are only able to measure the $|V\rangle$ and $|D\rangle$ states. We can simplify our operators and add a normalization factor

$$\widehat{M}_V = \sqrt{2}|V\rangle\langle V| \tag{11}$$

$$\widehat{M}_D = \sqrt{2}|D\rangle\langle D| \tag{12}$$

2.1 Altering the Measurement Basis

Measuring an entangled photon in the HV or DA basis collapses the state $|\psi\rangle$ and alters any further measurements of the other entangled photon. We will conduct three different tests, sending many pairs of entangled photons in the HV basis into two different detectors (Alice and Bob) which will measure if the photons are in the $|V\rangle$ or $|D\rangle$ state in the HV and DA basis respectively. We will assume that the pair is always measured first by Alice, though, the order of measurement does not change the results. We will record a coincidence count if both photons in a pair are measured as a "1" ($|V\rangle$ or $|D\rangle$) and record results for 120 seconds. We will not be attempting to predict the number of coincidence counts, rather, the number of coincidences relative to the counts in the baseline test, test 1.

Test 1 is measuring the entangled photon pairs in the HV basis at both detectors. At the first detector we measure the $|V\rangle$ state and therefore apply by $\widehat{M}_V$ to $|\psi\rangle$. Because we are measuring at Alice first, we notate the operator as $\widehat{M}_{V_s}$

$$\begin{aligned} \widehat{M}_{V_s}|\psi\rangle &= \sqrt{2}|V\rangle_s\langle V|_s\left(\frac{1}{\sqrt{2}}(|V\rangle_s|V\rangle_i + |H\rangle_s|H\rangle_i)\right) \\ &= |V\rangle_s(\langle V|_s|V\rangle_s|V\rangle_i + \langle V|_s|H\rangle_s|H\rangle_i)) \\ &= |V\rangle_s|V\rangle_i \end{aligned} \tag{13}$$

Then, at the second detector, the probability of measuring a "1" (V) can be found using

$$P_{V_i} = |\langle V|_i|\psi\rangle|^2 = |\langle V|_i|V\rangle_i|V\rangle_s|^2 = 1 \tag{14}$$

Note that we ignore the $|V\rangle_s$ because, while it is part of $|\psi\rangle$, it is not part of the photon that we are currently measuring. We will do this frequently while making our predictions. There is a 100% probability that we will measure a "1" at the second detector and therefore we will theoretically record 100% of the coincidence counts. The number of coincidence counts recorded in this test will be notated as X and used as the baseline for tests 2 and 3 which should be run immediately after.

Test 2 is measuring the entangled photon pairs in the HV basis at Alice and in the DA basis at Bob. Similar to test 1 we measure $|\psi\rangle$ in the HV basis first and collapse the state to

$$|\psi\rangle = |V\rangle_s|V\rangle_i \tag{15}$$

Then, at the second detector the probability of measuring a "1" (D) can be found using

$$P_{D_i} = |\langle D|_i|\psi\rangle|^2 = |\langle D|_i|V\rangle_i|V\rangle_s|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} \tag{16}$$

There is a 50% probability that we will measure a "1" at the second detector and therefore we will theoretically record 50% of the coincidence counts. Compared to test 1 this is $X/2$.

Test 3 is measuring the entangled photon pairs in the DA basis at Alice and at Bob. Note here that this scenario does not occur in the BB84 Protocol because Alice will always send out a photon in the basis in which they measured it, however, using our modified apparatus we can test it. At the first detector we measure the $|D\rangle$ state and therefore apply by $\widehat{M}_{D_s}$ to $|\psi\rangle$.

$$\widehat{M}_{D_s}|\psi\rangle = \sqrt{2}|D\rangle_s\langle D|_s\left(\frac{1}{\sqrt{2}}(|V\rangle_s|V\rangle_i + |H\rangle_s|H\rangle_i)\right) \tag{17}$$

And using equations 2 and 3

$$\widehat{M}_{D_s}|\psi\rangle = |D\rangle_s\langle D|_s\left(\frac{1}{\sqrt{2}}(|D\rangle - |A\rangle)|V\rangle_i + \frac{1}{\sqrt{2}}(|D\rangle + |A\rangle)|H\rangle_i\right) \tag{18}$$

$$= |D\rangle_s\left(\frac{1}{\sqrt{2}}(\langle D|_s|D\rangle - \langle D|_s|A\rangle)|V\rangle_i + \frac{1}{\sqrt{2}}(\langle D|_s|D\rangle + \langle D|_s|A\rangle)|H\rangle_i\right)$$

$$= |D\rangle_s\left(\frac{1}{\sqrt{2}}(|V\rangle_i + |H\rangle_i)\right)$$

$$= \frac{1}{\sqrt{2}}(|V\rangle_s|V\rangle_i + |H\rangle_s|H\rangle_i)$$

This is our original state $|\psi\rangle$. At the second detector the probability of measuring a "1" (D) can be found using

$$P_{D_i} = |\langle D|_i|\psi\rangle|^2 = \left|\langle D|_i\left(\frac{1}{\sqrt{2}}(|V\rangle_s|V\rangle_i + |H\rangle_s|H\rangle_i)\right)\right|^2 = \left|\frac{1}{\sqrt{2}}\left(\frac{1}{2} + \frac{1}{2}\right)\right|^2 = \frac{1}{2} \tag{19}$$

There is a 50% probability that we will measure a "1" at the second detector and therefore we will theoretically record 50% of the coincidence counts. Compared to test 1 this is $X/2$. We can summarize the results from the first three tests in Table 1.

Table 1: Summary of results of tests 1, 2, 3. Sending many pairs of entangled photons in the HV basis into two different detectors.

	Alice Measurement Basis	***Bob Measurement Basis***	***Coincidence Counts***
Test 1	HV	HV	X
Test 2	HV	DA	$X/2$
Test 3	DA	DA	$X/2$

These predictions agree with what was found experimentally in reference [6] However, they found that "[t]he agreement in the HV basis was greater than in the DA basis. This is likely due to not having perfect state fidelity. We implemented the setup and the experiment within the undergraduate laboratory context, with students (the first 2 authors) doing the alignments and the experiments." [6] We can expect to face similar difficulties and thus more error in test 3, where both measurements were made in the DA basis.

2.2 Adding an Eavesdropper

We will also perform three tests to investigate the effects of adding an eavesdropper (EVE) before Bob. The goal of the eavesdropper in the BB84 protocol is to measure the state of the photon from Alice and send it to Bob without altering the state. To do this, EVE must randomly choose the correct basis (HV or DA) to measure in. According to the BB84 protocol outlined in reference [5] if EVE chooses the correct basis, they will go unnoticed and 100% of the states passed on to Bob will be correct. However, if EVE chooses the wrong basis, 50% of the states passed on to Bob will be incorrect.

In reference [6], a Quartz plate is used to simulate EVE. If the quartz plate is at 0° relative to the detector (Bob), then entangled photons in the HV basis will pass through without being affected and EVE chose the correct measurement basis. If the quartz plate is rotated 45° the plate will delay one of horizontal or vertical components relative to the other enough so that they are decohered. This takes the $|H\rangle$ and $|V\rangle$ component of the state out of superposition and into a 'mixed' state where the photon is $|H\rangle$ half the time and $|V\rangle$ the other half [6]. Our three tests, (A, B, and C), will determine whether using a quartz plate in this matter produces the expected BB84 results. Each test will be done with Alice and Bob measuring in the HV basis.

Test A is the exact same as test 1 from earlier. EVE is not yet introduced to the system and the coincidence counts over 120 seconds will be recorded as a baseline and notated as Y.

Test B is adding the quartz plate (EVE) in the correct measurement basis (HV). The photons in state $|\psi\rangle$ will not be affected by the quartz plate and we can expect to record 100% of the coincidence counts. Compared to test A this is Y.

Test C is rotating the quartz plate 45° so that EVE is in the incorrect measurement basis (DA). First, we can rewrite $|\psi\rangle$ in terms of $|D\rangle$ to give us

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|D\rangle_s|D\rangle_i) \tag{20}$$

The quartz plate will decohere the photon which was headed towards Bob causing the state to change as such

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|D\rangle_s|D\rangle_i) \quad --EVE--> \quad |\psi\rangle = \frac{1}{\sqrt{2}}(|D\rangle_s(|V\rangle_i + |H\rangle_i)) \tag{21}$$

Where we can no longer write the idler photons in terms of $|D\rangle$ because they are not in a superposition. Now, when we measure $|\psi\rangle$ at Alice we get

$$\widehat{M}_{V_s}|\psi\rangle = \sqrt{2}|V\rangle_s\langle V|_s(\frac{1}{\sqrt{2}}(|D\rangle_s(|V\rangle_i + |H\rangle_i))) \tag{22}$$

$$= |V\rangle_s\langle V|_s\frac{1}{\sqrt{2}}(|V\rangle_s(|V\rangle_i + |H_s\rangle) + |H\rangle_s(|V\rangle_i + |H\rangle_i)))$$

$$= \frac{1}{\sqrt{2}}(|V\rangle_s(|V\rangle_i + |H_s\rangle)$$

Then, at the second detector the probability of measuring a "1" (V) can be found using

$$P_{V_i} = |\langle V|_i|\psi\rangle|^2 = \left|\frac{1}{\sqrt{2}}\langle V|_i|V\rangle_i|V\rangle_s\right|^2 = \frac{1}{2} \quad (23)$$

There is a 50% probability that we will measure a "1" at the second detector and therefore we will theoretically record 50% of the coincidence counts. Compared to test A this is $Y/2$. We can summarize the results from these three tests in Table 2.

Table 2: Summary of results of tests A, B, C. Sending many pairs of entangled photons in the HV basis into two different detectors with an eavesdropper being added.

	Alice Measurement Basis	***Bob Measurement Basis***	***EVE Measurement Basis***	***Coincidence Counts***
Test A	HV	HV	Not Included	Y
Test B	HV	HV	HV	Y
Test C	HV	HV	DA	$Y/2$

These predictions agree with what was found experimentally in reference [6].

3. Design of Apparatus

The apparatus was designed to split a single 405 nm photon to two 810 nm entangled photons. We used the coincidences between two detectors under different settings to determine whether photons are a secure medium for data transfer. The apparatus is shown below, refer to Figure 4.

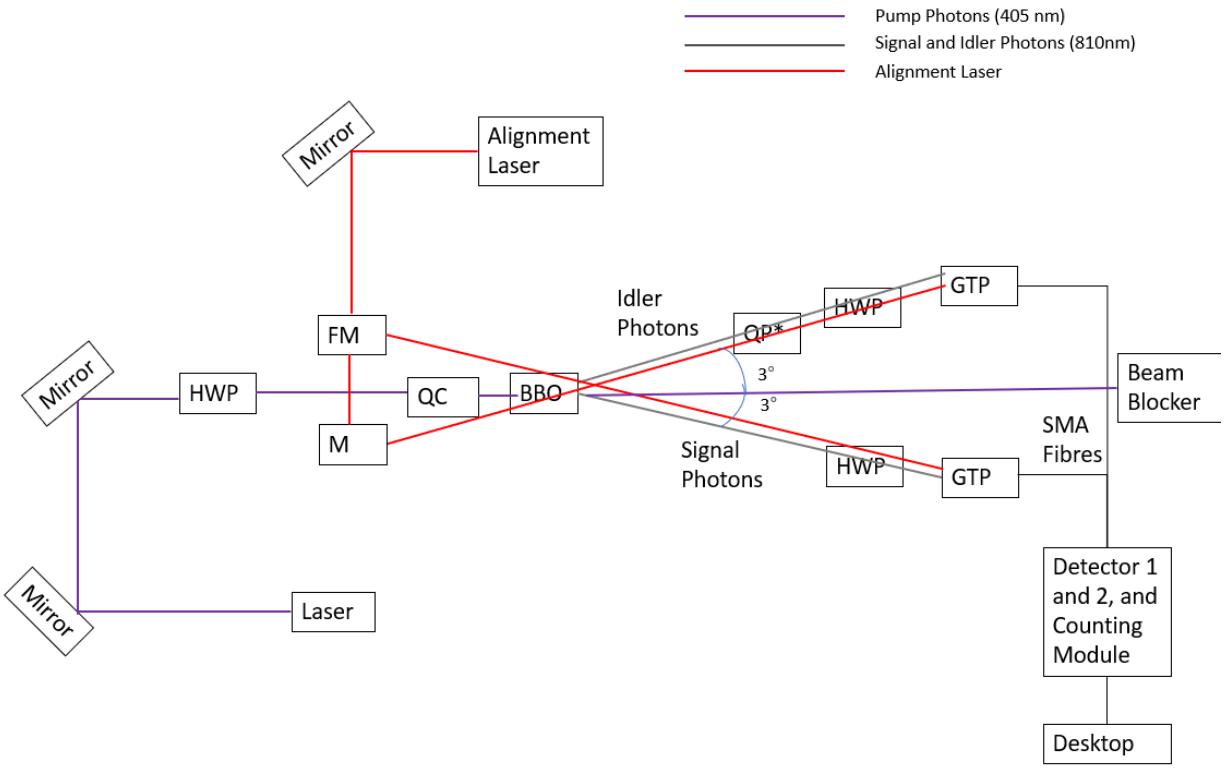

Figure 4: Experimental Apparatus used. Table below defines acronyms used in text blocks

All components listed as acronyms in Figure 4 are provided in the table below (Table 3)

Table 3: Acronyms in Figure 4

Acronym	Component
HWP	Half-Wave Plate
M and FM	Mirror and Flipper Mirror
QC	Quartz Crystal
BBO	Barium Borate Crystal
GTP	Glan-Thompson Polarizer
QP	Quartz Plate
SMA Fibre	Subminiature Version A Fibre

The apparatus can be thought of as several different apparatuses combined: the alignment laser, before the BBO crystal and after the BBO crystal. The following sections are described below.

3.1 Alignment Laser

The alignment laser was used to align optical components past the BBO crystal. This is because photons that are split by the BBO crystal are no longer visible (i.e., cannot view 810 nm).

The two Glan-Thompson polarizers that connect to the detectors are placed along an arc with a 1 m radius aligned to 3 degrees relative to the plane of the BBO crystal. 3 degrees is the angle which the signal and idler photons exit the BBO from.

The alignment laser hits two mirrors to align components in the plane with and without the quartz plate. Two mirrors were used to give vertical and horizontal freedom, to ensure that the beam is level. Since both mirrors are in the same plane, the flipper mirror was lowered to use the other mirror. We then ensured that the incident beams passed through the Glan-Thompson polarizers and could be viewed through the fibre. The half-wave plates were then placed in-line with the incident beam such that they passed through.

3.2 Before BBO Crystal

Prior to entering the BBO crystal, 405 nm vertically polarized photons are shot out of the laser. Again, two mirrors are used to provide two degrees of freedom (vertical and horizontal) to ensure that a level beam enters the BBO crystal.

Note that depending on the quality of the laser, polarizers can be placed between the mirrors to increase the polarization quality of the light emerging from your laser. During our testing we found that the polarizers had an insignificant effect on photon detection, and we opted to remove them.

After the photons are leveled by the mirrors, they go through a half-wave plate set to 22.5 degrees. The half-wave plate is used to rotate the emerging light to either the HV or DA basis. The quartz plate is used to align the phase of both components of either state (i.e., aligning cones the exit the BBO as described previously).

3.3 After (and including) BBO Crystal

The BBO crystal splits the single 405 nm photon into a pair of entangled 810 nm photons. The mechanism responsible for this is spontaneous parametric down conversion. This is a non-linear optical process that converts a single photon of higher energy into two photons with half the energy and double the wavelength [7].

When the quartz plate is not in the setup both photons pass through a half-wave plate and Glan-Thompson polarizer tuned to 810 nm. The two half-wave plates rotate the photons to one of either the

HV or DA measurement basis depending on the angle they are set to. The Glan-Thompson polarizer lets in light at the angle that it is set to.

The quartz plate acts as the eavesdropper (Eve) and retards the light causing the pair of photons to be decoherent, therefore altering the number of coincidences.

Individually the photons pass through an SMA fibre to a detector, and if they both reach the detector within 40 ns, they are considered a coincidence. Otherwise, they are marked only as a detection and not a coincidence.

3.4 Sensitivity of Components

Due to the nature of this experiment, it is imperative that alignment is done correctly. Poor alignment can result in photons being outside the accepting angle of the fibre and therefore going undetected. Additionally, surfaces not being perfectly level could have resulted in some photons exiting at paths that would never meet the detector. The detectors do not have a 100% detection rate, and resultantly all photons that reached the detector were not necessarily detected.

3.5 Safety Considerations

The laser is high powered and classified as 3B, to ensure maximal safety we wore optical glasses that minimized the intensity of light such that it would not damage our eyes. Additionally, a beam block was placed in the plane of the BBO to absorb photons that are not split. Throughout the experiment beam blocks were used to capture incident beams so that no one was injured.

4. Procedure

4.1 Coincidence Counter and Altera

A MATLAB program was used to collect data as well as display the results from the setup. Using a fibre optic cable, photons were sent from the Glan-Thompson Polarizers to their respective detectors. The original experiment and analysis had to be modified to account for only having two single photon detectors instead of four as described in the original experiment. Since we could now only measure a portion of the photons emitted from the BBO crystal, we could not implement the BB-84 protocol and do the full cryptography setup. Instead, we tested if we could detect the presence of an eavesdropper to determine whether photons are a safe medium for encryption. The two-detector setup is limited to only counting increases and decreases in coincidence counts which can then be compared to expected values by percentage of a baseline. The output signal from the detectors was connected as a digital signal to an Altera FPGA. Photon counts were converted to a digital spike in voltage, counted and summed using a MATLAB program.

By configuring the Altera pins to the correct states, different counts for LOW or HIGH were detected, so that coincidences could be counted. The following pin configuration in Figure 5, was used allow data flow and get readings in the program. This setting could be used for up to four detectors.

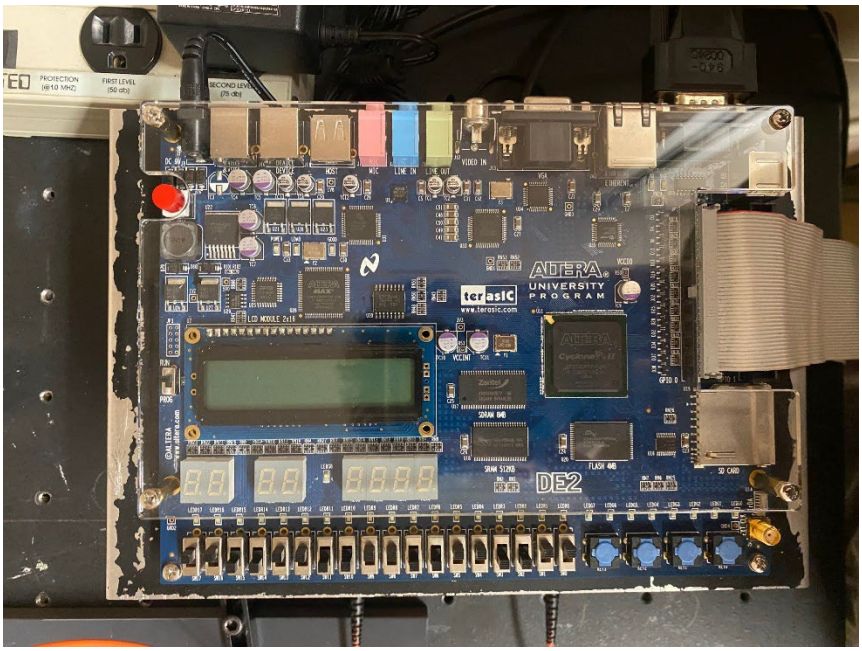

Figure 5: Correct Altera Pin setup to measure coincidences in 2 detectors. A and B.

These pin states allow the detection of single photons using two detectors A and B as well as counting coincidences between the two. Accidentals were measured and subtracted from the total coincidence counts. It is expected that for larger counts on detectors and coincidences the accidentals will increase proportionally. This data is written to CSV and can be exported to perform further analysis.

The necessary pin states on the Altera can be determined by following this logic. Every four pins dictate the counting state of a detector with the first two on the far left being single counts. For every new counter, two pins must be set to HIGH which will determine which two states are being compared and the other two must be set LOW. An example setup can be found in Figure 6.

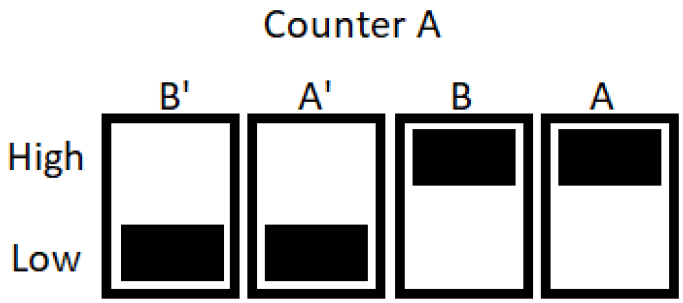

Figure 6: Following the logic explained above, Counter A would be counting AB coincidences.

Notable sections from the MATLAB program can be found in the appendix. The program acts as a repeated counter which takes sample points at the designated time intervals. Accidentals are calculated and subtracted from the total coincidence count before data is analyzed.

4.2 Laser and BBO Alignment

The first step in setting up the apparatus was laser alignment. The first step in this process was determining the positions of the detectors and the BBO crystal. The BBO ejects the photons at a three-degree angle from the center line, so the detectors must be directly on these angles. A backboard with a circular edge, radius one meter, was placed on one end of the table. A location for the BBO crystal was found using the intersection of lines orthogonal to the backboard. The location for the detectors also needed to be determined. Using trigonometry, it was found that at one meter, a three-degree displacement corresponds to $5.2\ cm$. Now that the components were placed the next step was aligning the lasers.

The difficulty is that the BBO only splits a small fraction of the photons from the blue laser, and they are at a wavelength not visible to the human eye. Therefore, we had to use a red alignment laser. Since two degrees of freedom were needed, the red laser was redirected by three mirrors, one for vertical alignment and two for each three-degree horizontal angle. The height of the detectors is fixed so the first mirror was used to align the laser to the detector height. The second two mirrors were used to align the light to each three-degree angle. The laser is in the correct position when it passes through the center of the BBO and hits the center of the detector. Using trial and error, the location and angle for each mirror was found and aligned. One mirror had to be a flipper mirror so that both angles could be seen and so that we could flip between both photon paths. Finally, the detectors were aligned to directly point at the BBO crystal by taking one end of the fiber optic cable out and maximizing its output.

The next step was aligning the blue light. A similar process with two mirrors was used to align the laser to the center line. The correct position was when the laser passed through the BBO and hit the center line at the height of the detectors. Now that the laser paths were not visible, the MATLAB program was used to display the counts and coincidences. A systematic approach was used to find the alignment positions. By incrementally varying the alignment axis of a component we could look at the counts or coincidences and find a maximum. The component would be set to that angle for that axis and the process was repeated for each axis until all axes were aligned. An example of what this looked like can be found in the figure below.

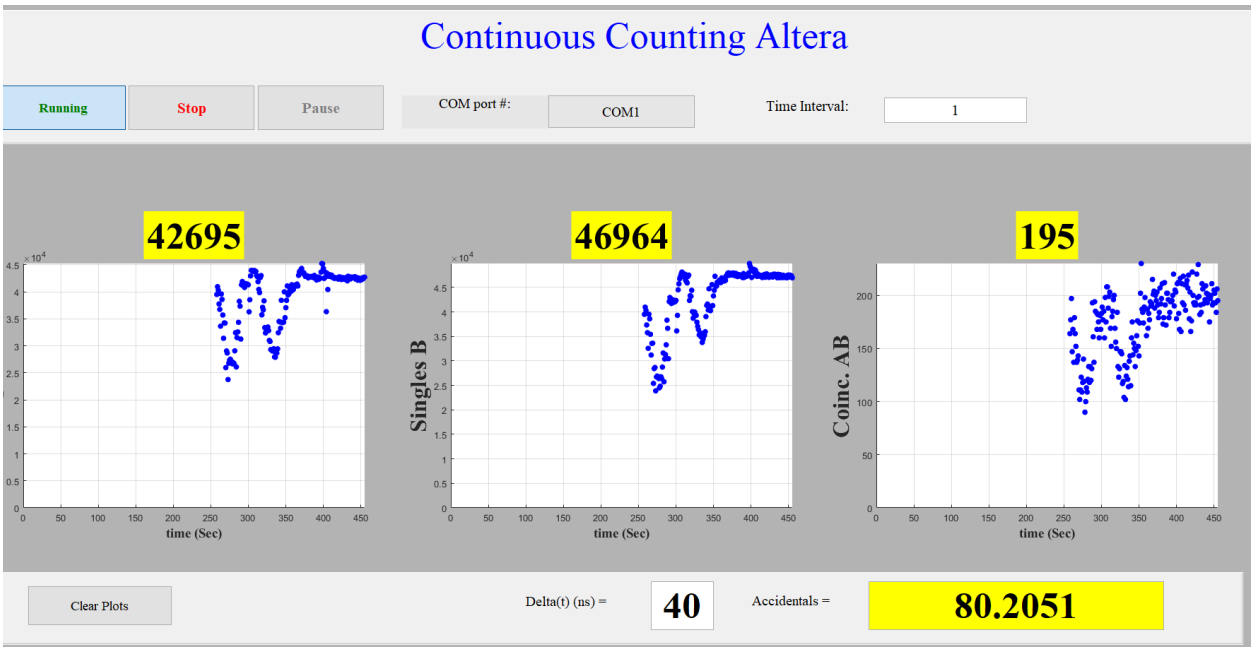

Figure 7: MATLAB plot of alignment process. The angle of the BBO was swept until a maximum was found and the angle was rotated back to achieve alignment in the axis.

These plots were for the alignment of z axis rotation of the BBO crystal. When the component was at the best alignment, the detections were at a peak. The angle was then brought back to where the detections were maximized. This process was repeated for all axes of the BBO crystal and both detectors.

4.3 Component Setup and Alignment

A similar process was used to set up and align all the other optical components. We placed and aligned each component individually and did a series of tests to ensure the components were doing what we expected.

First, we put in the polarizers. We set them to the zero angle but realized that they were blocking more light than expected and each one was blocking a different amount of light. This led us to believe that the polarizers were not aligned exactly to the laser or to each other. The angle we wanted the polarizers at was in the same polarization angle emitted from the laser. When the polarizers are at this angle the detection will be at a maximum so the process in Figure 7 was used. The alignment of the first polarizer was at roughly $17°$ and the other at roughly $52°$. After comparing the outputs of the counter and coincidences we saw that the polarizers had little to no effect because the laser output was already well attenuated, so we decided not to use them.

Next, we put in the half wave plate to rotate the polarization of the light. We wanted the light to be rotated $45°$, so we turned the half wave plate to half the desired rotation amount, $22.5°$. We did a test using the polarizers to confirm that this rotated the polarization by the desired amount. Then we put in the Glan-Thompson Prisms and aligned them using our alignment technique and rotated the polarization to align with the correct basis. Similarly, the second halfwave plates were placed in front of the TP's for selecting the basis. Finally, we used the quartz plate and our alignment technique to shift the cones emitted from the BBO, causing the superposition, and maximizing coincidences.

We then ran all the desired tests. A summary of the tests and how they were completed can be found in the data section below.

5. Data

All data is collected using the MATLAB program for a variety of different polarizing and half wave plate setups. Each dataset is run for 120 seconds and sampled in 5 second intervals. The time interval for coincidences is set to 40 nanoseconds to account for accidental counts and maximize the coincidences in our apparatus

Six different setups are tested to confirm predictions. Tests 1 through 3 refer to the baseline maximum count where no quartz plate is introduced. Tests A through C are for the baseline scenario where the quartz plate in alternating basis is introduced. The angle of rotation of each component per test is summarized in the table below.

Table 4: Summary of all six test cases and corresponding rotation of optical components.

	HWP 1	HWP A	HWP B	Quartz Plate
Test 1	22.5°	0°	0°	No
Test 2	22.5°	22.5°	0°	No
Test 3	22.5°	22.5°	22.5°	No
Test A	22.5°	0°	0°	No
Test B	22.5°	0°	0°	0°
Test C	22.5°	0°	0°	45°

All tests are conducted in the HV basis as the correct basis and DA as the incorrect basis. It can be expected that the DA basis will also return similar results if treated as the correct basis and vice versa. Test 1 is for coincidences with both HWP's in the correct basis. Test 2 is a test of coincidences where only one HWP is in the HV basis. Test 3 is a test where both HWP are in the incorrect basis. Test A is for both HWP in the correct basis without an eavesdropper to create a new baseline model. Test B is for coincidences where both HWP are in the correct basis as well as the eavesdropper. The final test is a similar case but instead the quartz plate is in the incorrect basis. The preliminary data collected for Tests 1 through 3 are shown below.

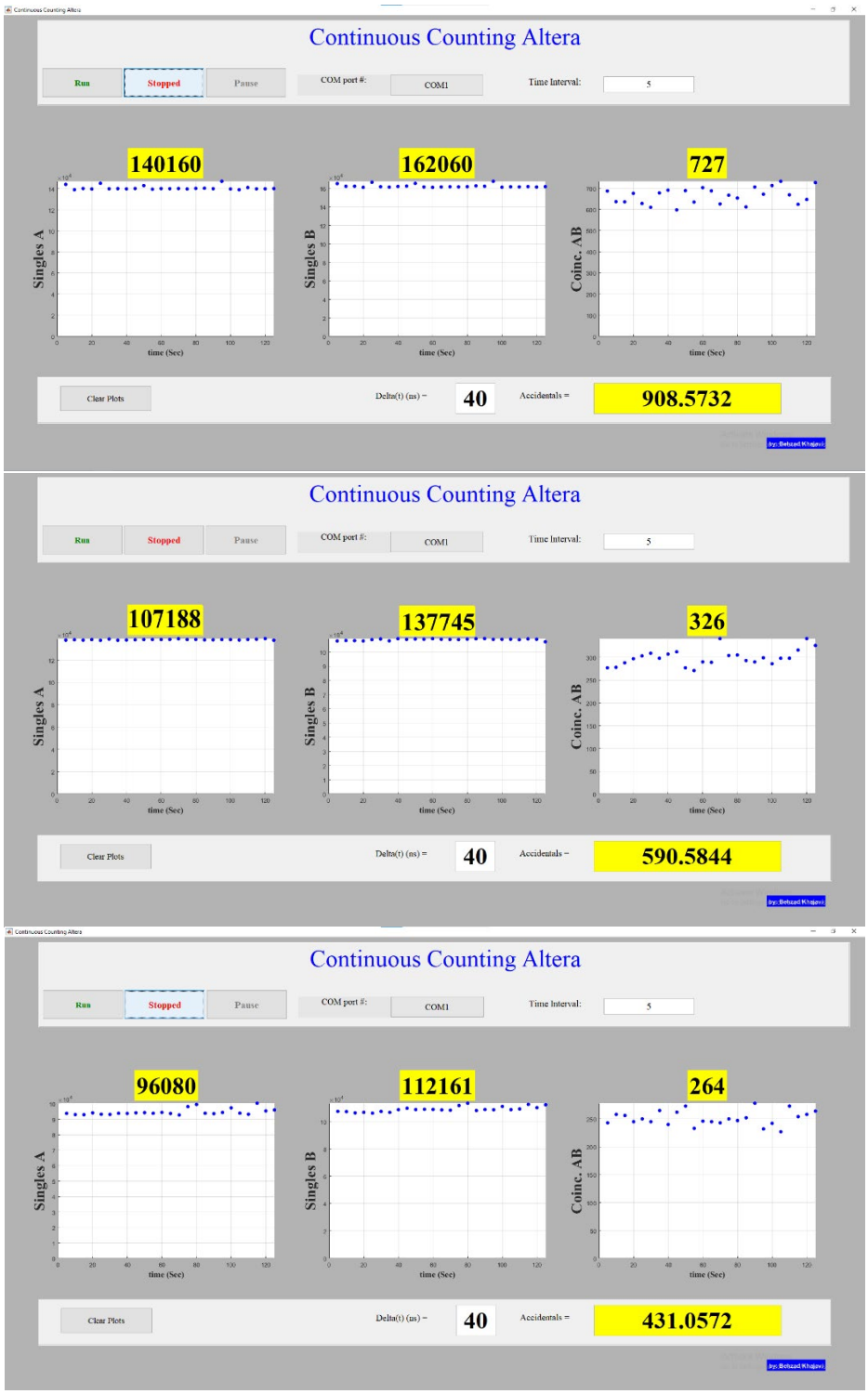

Figure 8: Preliminary data corresponding to tests 1-3 respectively. Can be compared to mathematical results to further confirm predictions. Note that these results displayed are not averaged.

From experimentation, uncertainty is considered for coincidence counts between A and B. By referencing the MATLAB code and counting of the accidentals, the error analysis is already encompassed in the accidental count and will automatically be subtracted from the total coincidence counter. Additionally,

for smaller fluctuations in counts the error is mitigated by having each trial run for 120 seconds and averaging each point.

```
%% Calculating and then Showing Accidentals

deltat=str2double(get(handles.Deltatedit7,'String'));
acc=numofcountsA*numofcountsB*deltat*0.000000001;
```

Figure 9: Accidental calculation which encompasses the error expected from experimental uncertainties.

6. Analysis

By comparing the coincidences between trials, we did not see the expected results for a few tests. We found that there was an error in the methodology we used to compare results between trials. To better analyze the data and try to understand what was happening in each test, we needed to extract a "relative coincidence count" which we will call the N value. We define the variable N to be the ratio of coincidences to the maximum possible in the trial. The maximum number of possible coincidences, given the returned counts from detectors A and B, is the lesser of the two counts. By finding the N value of each test we can compare the ratio of each N to determine the effect the changes made to the optical equipment in each test. The N value does not describe all information needed for the analysis but serves as a baseline method to compare between trials.

Also, the standard deviation will be used as a quantitative error estimate. This error estimate captures sources of error such as dust in the air and random lost detections but does not factor in sources of error such as alignment of lasers and components. The python uncertainties library was used to propagate error. The code can be found in the Appendix.

6.1 Altering the Measurement Basis

6.1.1 Test 1

To model Alice and Bob both in the correct basis, their half wave plates were oriented to the HV basis. The test was run for two minutes, and the data was averaged to give the following results.

Table 5: Average counts in A, counts in B, and coincidences AB for Test 1

Counts A	138793 ± 956
Counts B	162720
Coincidences AB	664 ± 37

In this test the N value is the ratio of Counts A, the lesser of the two counts, to the Coincidences AB

$$N_1 = \frac{Coincidences\ AB}{Counts\ A} = \frac{664}{138793} = (0.48 \pm 0.05)\%$$

In this test, N serves as a baseline comparison for the next two tests. The error is calculated to be

6.1.2 Test 2

Test 2 simulates Alice being in the correct basis and Bob in the wrong one. Bob's half wave plate was rotated to align him to the DA basis. Running the simulation and averaging the data gave the following results.

Table 6: Average counts in A, counts in B, and coincidences AB for Test 2

Counts A	138160 ± 366
Counts B	108720
Coincidences AB	300 ± 17

In this test,

$$N_2 = \frac{Coincidences\ AB}{Counts\ B} = \frac{300}{108702} = (0.28 \pm 0.02)\%$$

The expected result was that the coincidences would reduce by 50% for this test. By comparing the N values,

$$\frac{N_2}{N_1} = \frac{0.28\%}{0.48\%} = (58 \pm 5)\%$$

This is not exactly what we were expecting but given the uncertainty in the alignment and the rotation angles of the components this result was satisfactory accounting for the standard deviation error we are withing 3% of our prediction and the remaining error can be attributed qualitatively to errors in alignment and calibration.

6.1.3 Test 3

Test 3 simulates both Alice and Bob in the wrong basis. This was done by rotating Alice and Bob's half wave plates to the DA basis. The averaged test results are as follows.

Table 7: Average counts in A, counts in B, and coincidences AB for Test 3

Counts A	94709 ± 1971
Counts B	108920
Coincidences AB	251 ± 12

Calculating the N value,

$$N_3 = \frac{Coincidences\ AB}{Counts\ A} = \frac{251}{94709} = (0.27 \pm 0.01)\%$$

The expected result was that the coincidences would also reduce by 50% for this test. By comparing the N values,

$$\frac{N_3}{N_1} = \frac{0.27\%}{0.48\%} = (55 \pm 4)\%$$

Again, this is not exactly what we were expecting, but factoring in the error the result was within 1% of the expected. Further we were expecting no change between tests 2 and 3.

$$\frac{N_3}{N_2} = \frac{0.27\%}{0.28\%} - 1 = (4 \pm 7)\%$$

The N values were off by a factor of only 4%. This ratio indicates that there was something misaligned in the setup. Otherwise, the values are as predicted.

A summary of the results found by altering the measurement basis is shown in Table 8:

Table 8: Summary of results for the tests altering the measurement basis compared to the predictions

	Alice Measurement Basis	***Bob Measurement Basis***	***Coincidence Counts Prediction***	***N-Value Ratio***
Test 1	HV	HV	X	N
Test 2	HV	DA	X	$0.58N$
Test 3	DA	DA	$0.5X$	$0.56N$

6.2 Adding an Eavesdropper

6.2.1 Test A

Test A is the same as Test 1, simulating Alice and Bob in the correct basis. This test was needed because the remaining tests were performed on a different day than the previous and the optical alignment may have shifted. The average data for the detections is as follows.

Table 9: Average counts in A, counts in B, and coincidences AB for Test A

Counts A	145880 ± 1211
Counts B	183600
Coincidences AB	806 ± 29

The baseline N value for this test is,

$$N_A = \frac{Coincidences\ AB}{Counts\ A} = \frac{806}{145880} = (0.55 \pm 0.02)\%$$

6.2.2 Test B

Test B introduces the eavesdropper where she is first in the correct basis (HV). This is done by putting the quartz plate perpendicular to the laser in front of Alice's detector. Averaging the data from the two-minute test resulted in the following.

Table 10: Average counts in A, counts in B, and coincidences AB for Test B

Counts A	142480 ± 805
Counts B	182240
Coincidences AB	778 ± 32

The N value for this test is,

$$N_B = \frac{Coincidences\ AB}{Counts\ A} = \frac{778}{142480} = (0.55 \pm 0.02)\%$$

Exactly as expected, this test does not affect the N values,

$$\frac{N_A}{N_B} = \frac{0.55\%}{0.55\%} = (99 \pm 5)\%$$

6.2.3 Test C

The final test simulates the eavesdropper guessing the wrong basis (DA). This was implemented by placing the quartz plate at a $45°$ angle to the laser line. The results are as follows.

Table 11: Average counts in A, counts in B, and coincidences AB for Test C

Counts A	71985 ± 3565
Counts B	164000
Coincidences AB	155 ± 11

$$N_C = \frac{Counts\ A}{Coincidences\ AB} = \frac{155}{71985} = (0.55\%$$

In this test we see a good example of why the N value was necessary. The prediction of coincidences was way off from the expected 50%.

$$\frac{Test\ B\ Coincidences\ AB}{Test\ A\ Coincidences\ AB} = \frac{155}{806} = (19 \pm 2)\%$$

Where as comparing N values,

$$\frac{N_A}{N_C} = \frac{0.55\%}{0.22\%} = (40 \pm 4)\%$$

7. Discussion and Future Work

7.1 Results

To analyze our experiment and validate our apparatus, we iterated through several tests with different measurement bases, and tested with and without Eve.

The most important of these tests were the following:

- Test B, coincidences with both measurements in the correct basis, and Eve in the correct basis
- Test C, coincidences with both measurements in the correct basis and Eve in wrong basis

This is because we expect to see an approximately 50% drop in coincidences due to the decoherence of the qubit state caused by the quartz plate. This would indicate a successful implementation of the first stage of the BB84 protocol. Through the observation of these coincidence counts, it was determined we were successful in detecting the presence of an eavesdropper, however there was some error in the exact decrease in counts

Average counts per second over 125 seconds:

No Eavesdropper:

$$806 \pm 29\ counts$$

Eavesdropper in Alice-Bob Basis:

$$778 \pm 32\ counts$$

Eavesdropper in wrong Basis:

$$155 \pm 11\ counts$$

To account for various losses at each step, we did this analysis with ratios of N-values as described in the analysis section.

$$\frac{N_A}{N_C} = \frac{0.55\%}{0.22\%} = (40 \pm 4)\%$$

This is not exactly the 50% which we expected, however does agree within approximately two standard deviations. Because of the difficulty in modelling losses at each state of the apparatus, this was deemed acceptable. The coincidences do not factor in the large reduction in possible coincidences due to the reduction in Counts A. This result was the furthest off from our predictions. It is roughly what we expected, 6% off when factoring in error. There is the highest possible chance of error due to optical alignment for this test, so it is possible that this is what caused the deviation. For example, we had no way of knowing when the quartz plate was at exactly 45°. A small error in this angle could be responsible for the reduction in counts. Another possible source of error is the refraction of the laser caused by the quartz plate. Further tests would have to be done to confirm where exactly the remaining error came from. A summary of the results found with the addition of an eavesdropper is shown in Table 12.

Table 12: Summary of results for the tests with the eavesdropper compared to the predictions

	Alice Measurement Basis	***Bob Measurement Basis***	***Eve Measurement Basis***	***Coincidence Counts***	***N-Value Ratio***
Test A	HV	HV	Not Included	Y	N
Test B	HV	HV	HV	Y	$0.99N$
Test C	HV	HV	DA	$0.5Y$	$0.4N$

Here, the Alice-Bob basis of the quartz plate corresponds to the quartz plate being perpendicular to the incident beam. This leaves the photons unaffected and results in Alice and Bob measuring the same result. However, if the Quartz crystal is at an angle to the incident beam, this results in the photons interacting with the crystal, and breaking the entanglement between the states. This means that Alice and Bob will become uncorrelated and probabilistic making the data of no use in a private key.

7.2 Future Work

To improve the quality of our results, more time could have been spent optimizing coincidences. This would involve additional alignment and tuning of filter angles. One limitation of the experiment was that there were only two single photon detectors available instead of the desired four. Four single photon detectors would have allowed for a full implementation of the BB84 protocol and for sample key distributions where bits could be measured for both Alice and Bob. The first extension to the experiment would be this full implementation. After this, an additional improvement which could be made is the use of fiber optic cables throughout each state of the apparatus to eliminate the need for the photons to travel freely through the air. This would bring the experiment one step closer to a practical implementation, however, would require significant changes to filter types, BBO housing and more.

8. Conclusions

When Alice and Bob measure in the same basis and no eavesdropper is in the system, we observed 0.48% of the maximum coincidences. When there is no eavesdropper and either Alice or Bob operates in the wrong basis the relative coincidences drop by approximately 42%. We observed that if both Bob and Alice operate in the wrong basis, then relative coincidences drop by 44%. The introduction of an eavesdropper can go undetected if placed in the correct basis; however, when in the wrong basis the relative coincidence count drops by 60%. We found that the error we could classify quantitively, standard deviation between measurements, was not enough to bring us to our predictions. However, when factoring in qualitative estimations from uncertainties in surfaces of optical components and detector efficiency our results are within a good range of the predictions. Therefore, our experiment demonstrates that the introduction of a quartz plate (i.e., eavesdropper) can be detected when it is in the incorrect basis. Thus, entangled photons are a safe medium for data transfer.

10. Appendix

```
    %% Calculating and then Showing Accidentals


    deltat=str2double(get(handles.Deltatedit7,'String'));
    acc=numofcountsA*numofcountsB*deltat*0.000000001;
    pause(0.01);
   strcat('Pausebuttonvalue in Pause push button->',num2str(pausebuttonvalue));
    if mod(pausebuttonvalue,2) == 0
%% plotting the data points on different subplots
    time = time + timeinterval; % x-axis (time) in seconds
    % plotting A
    axes(handles.axes1);
    plot(time,numofcountsA,'. b','MarkerSize',20);
    descriptionA = num2str(numofcountsA);
    title(descriptionA,'FontWeight','bold','FontSize',40,'FontName','Times New Roman')
    set(get(gca,'title'),'background','y')
    xlabel({'time (Sec)','',''},'FontWeight','bold','FontSize',14,'FontName','Times New Roman');
    ylabel('Singles A','FontWeight','bold','FontSize',25,'FontName','Times New Roman');

    %%%%%%%%%%%%%%%%%%%%%%
    % plotting B
    axes(handles.axes2);
    plot(time,numofcountsB,'. b','MarkerSize',20);
    descriptionB = num2str(numofcountsB);
    title(descriptionB,'FontWeight','bold','FontSize',40,'FontName','Times New Roman')
    set(get(gca,'title'),'background','y')
    xlabel({'time (Sec)','',''},'FontWeight','bold','FontSize',14,'FontName','Times New Roman');
    ylabel('Singles B','FontWeight','bold','FontSize',25,'FontName','Times New Roman');
    %%%%%%%%%%%%%%%%%%%%%%
    % plotting AB
    axes(handles.axes3);
    plot(time,numofcountsAB,'. b','MarkerSize',20);
    descriptionAB = num2str(numofcountsAB);
    title(descriptionAB,'FontWeight','bold','FontSize',40,'FontName','Times New Roman')
    set(get(gca,'title'),'background','y')
    set(handles.accidentalsedit6,'String',num2str(acc))%displays accidentals (here to be simultaneously shown)
    drawnow
    xlabel({'time (Sec)','',''},'FontWeight','bold','FontSize',14,'FontName','Times New Roman');
    ylabel('Coinc. AB','FontWeight','bold','FontSize',25,'FontName','Times New Roman');
```

```
% while get(hObject,'Value')
    count=count+1;
    myDatadimension=41*(timeinterval*10)+40; % timeinterval*10=timeinterval in seconds
    cleandatadimension=41*(timeinterval*10);
    myData=zeros(myDatadimension,1);
%   Serial data acquisition
    for i=1:timeinterval
         myData1 = fread(s,512,'uint8'); % reading # of bytes
         myData(1,(i-1)*512+1:i*512) = myData1';
    end
    % finding terminationbyte if the 41th element of myData is not 255
    tbi=0;
    if myData(1,41)~=255
        for i=1:40
           if myData(1,i)==255
               terminationbyteindex=i;
           end
        end
        tbi=terminationbyteindex;
    end
    cleandata=myData(1,tbi+1:tbi+cleandatadimension);
    numofcounts=zeros(1,8);
    CD=cleandata; % just to use a shorthand notation CD
    kmax=timeinterval*10; % loop repetation number for each counter
    L=0;

    for i=1:8
        j=0;
        for k=1:kmax
            numofcounts(1,i)=numofcounts(1,i)+CD(1,1+j+L)+2^7*CD(1,2+j+L)+2^14*CD(1,3+j+L)+2^21*CD(1,4+j+L)+2^28*CD(1,5+j+L);
            j=j+41; % the corresponding figure after a tenth of a second
        end
        L=L+5; % next counter partition starts at the next 5th byte
    end
    numofcountsA = numofcounts(1,1);
    numofcountsB = numofcounts(1,2);
    numofcountsAB = numofcounts(1,5);
    dlmwrite('dataaa16A.csv', numofcountsA, '-append')
    dlmwrite('dataaa16B.csv', numofcountsB, '-append')
    dlmwrite('dataaa16AB.csv', numofcountsAB, '-append')
```

Figure 10: Code snippet from coincidence counter program in MATLAB

```
from uncertainties import *

Coinc1 = ufloat(664, 37)
Counts1 = ufloat(138793, 956)
N1 = (Coinc1*100)/Counts1


Coinc2 = ufloat(300, 17)
Counts2 = ufloat(108720, 366)
N2 = Coinc2*100/Counts2

Coinc3 = ufloat(251, 12)
Counts3 = ufloat(94709, 1971)
N3 = Coinc3*100/Counts3

Coinc4 = ufloat(806, 29)
Counts4 = ufloat(145880, 1211)
N4 = Coinc4*100/Counts4

Coinc5 = ufloat(778, 32)
Counts5 = ufloat(142480, 805)
N5 = Coinc5*100/Counts5

Coinc6 = ufloat(155, 11)
Counts6 = ufloat(71985, 3565)
N6 = Coinc6*100/Counts6

Error2 = N2/N1
Error3 = N3/N1
Error35 = N3/N2-1
Error2 = N5/N4
Error2 = Coinc6/Coinc4
Error2 = N6/N4
```

Figure 10: Further error propagation for uncertainty in detections.

11. Acknowledgements

We would like to acknowledge the ENPH353 teaching team and our gratitude towards them. We give special thanks to Dr. Svetlana Kostina, Cameron Romanet, and Dr. Robert Knobel for their support throughout this experiment. As well, we would like to credit Dr. Behzad Khajavi for writing the MATLAB code used in this experiment.

12. References

[1] C. Dong, In *Math in Network Security: A Crash Course*, Chapter 6: Discrete Logarithms, course notes, [Online]. Available: https://www.doc.ic.ac.uk/~mrh/330tutor/ch06s02.html#:~:text=The%20discrete%20logarithm%20problem%20is,logarithms%20depends%20on%20the%20groups [Accessed 28 September 2022]

[2] Charlie Bennett, Lev Bishop, Sergey Bravyi, Andrew Cross, Jay Gambetta, Paul Nation, John Smolin, Kristan Temme and Abby Cross, In *IBM Quantum Composer*, Shor's algorithm, IBM Quantum Composer 2021 [Online] https://quantum-computing.ibm.com/ [Accessed 11 October 2022]

[3] Bacciagaluppi, Guido, "The Role of Decoherence in Quantum Mechanics", The Stanford Encyclopedia of Philosophy (Fall 2020 Edition), Edward N. Zalta (ed.) [online] https://plato.stanford.edu/archives/fall2020/entries/qm-decoherence/

[4] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters,* vol. 85, no. 2, pp. 441-444, 2000. https://doi.org/10.1103/PhysRevLett.85.441

[5] Y. Bloom, I. Fields, A. Maslennikov and G. Rozenman, "Quantum Cryptography - A Simplified Undergraduate Experiment and Simulation," *Physics,* vol. 4, p. 104-123, 2022. https://doi.org/10.3390/physics4010009

[6] A. Bista, B. Sharma and E. J. Galvez, "A Demonstration of Quantum Key Distribution with Entangled Photons for the Undergraduate Laboratory," American Journal of Physics 89, 111 (2021); https://doi.org/10.1119/10.0002169

[7] J. Bordy, "Quantum Entanglement (WOW!)," Quantum entanglement lab manual, Emory University, 2019 [Online]. Available: https://physics.emory.edu/faculty/brody/Advanced%20Lab/entanglement%20manual.pdf. [Accessed 28 September 2022].